(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number: **0 234 100 B1**

(12) # EUROPEAN PATENT SPECIFICATION

(45) Date of publication of patent specification: **15.01.92**

(51) Int. Cl.5: **G07F 7/10, G06F 7/58**

(21) Application number: **86309239.1**

(22) Date of filing: **26.11.86**

(54) **Method and apparatus for synchronizing the generation of separate, free-running, time-dependent codes.**

(30) Priority: **27.11.85 US 802579**

(43) Date of publication of application:
02.09.87 Bulletin 87/36

(45) Publication of the grant of the patent:
15.01.92 Bulletin 92/03

(84) Designated Contracting States:
AT BE CH DE ES FR GB GR IT LI LU NL SE

(56) References cited:
EP-A- 0 010 496
EP-A- 0 140 013
WO-A-85/04035
US-A- 3 764 742
US-A- 4 320 387

IBM TECHNICAL DISCLOSURE BULLETIN, vol. 26, no. 7A, December 1983, pages 3292-3293, New York, US; R.E. LENNON et al.: "Composite time-variant random numbers"

IBM TECHNICAL DISCLOSURE BULLETIN, vol. 26, no. 7A, December 1983, pages 3286-3288, New York, US; R.E. LENNON et al.: "Transaction response message authentication"

(73) Proprietor: **Security Dynamics Technologies Inc.**
2067 Massachusetts Avenue
Cambridge Massachusetts 02140(US)

(72) Inventor: **Weiss, Kenneth P.**
15 Dwight Street
Boston Massachusetts 02109(US)

(74) Representative: **Read, Matthew Charles et al**
Venner Shipley & Co. 368 City Road
London EC1V 2QA(GB)

Description

The present invention relates to an apparatus and method for the electronic generation of variable, non-predictable codes and the validation and comparison of such codes for the purpose of positively identifying an authorised individual or user of an apparatus or system.

There often arises a need to prevent all but selected authorised persons from being able to carry out some defined transaction (such as granting credit) or to gain access to electronic equipment or other system, facility or data (hereinafter "clearance or access"). Prior methods for preventing unauthorised clearance or access typically involve devices which limit access to the subject data, facility, or transaction to those who know a fixed or predictable (hereinafter "fixed") secret code. The problem inherent in relying on a fixed code as the means to gain such selective clearance or access is that would-be unauthorised users need only obtain possession of the fixed code to gain such clearance or access. Typical instances of fixed codes include card numbers, user numbers or passwords issued to customers of computer data retrieval services.

A known apparatus and method for providing security in financial transactions is disclosed in US 4320387. Security in transactions between separate computers associated with respective individuals is ensured by a system for comparing and matching non-predictable codes generated by the separate computers, comprising: a first computer, operable to produce a first non-predictable code on the basis of a first dynamic variable and a static variable; a first clock means for defining the first dynamic variable, according to a first interval of time during which the static variable is input into the first computer; a second computer, operable to produce a second non-predictable code on the basis of a second dynamic variable and the static variable; a second clock means for defining the second dynamic variable, according to a second interval of time during which the static variable is input into the second computer; and means for comparing the first non-predictable codes with the second non-predictable codes to determine a match.

Likewise, security is ensured by a method for synchronising the time definition of dynamic variables in a system for comparing non-predictable codes generated by separate clock means according to time wherein the codes match when the dynamic variables match, comprising the steps of: inputting a static variable into a first computer including a predetermined algorithm; employing the algorithm of the first computer to calculate a first non-predictable code on the basis of the static variable and a first dynamic varible defined by a first interval of time in which the step of inputting occurred according to a first clock; putting the static variable and the first non-predictable code into a second computer independently including the predetermined algorithm; using the algorithm of the second computer to independently calculate a second non-predictable code on the basis of the static variable and a second dynamic variable defined by a second interval of time in which the step of inputting occurred according to a second clock means; and comparing a first non-predictable code with a second non-predictable code to determine a match.

WO85/04035 discloses a portable transaction device for use in a transaction system. The device includes a computer and means to encrypt transmission data as a function of clock information.

With apparatus and a method of this kind it is necessary for the clocks of the two computers to be reasonably synchronised for the non-predictable codes to match. WO85/04035 makes no detailed disclosure of how this might be achieved. US4320387 discloses the use of a synchronisation code, transmitted between the parties of a transaction.

The present invention is intended to overcome the disadvantages of the prior art by the provision, according to a first aspect, of a system, wherein the second interval of time comprises a central cell of time, having a predetermined duration, and one or more cells of time, each having a predetermined duration, bordering the central cell, and the second clock means defines respective values of the second dynamic variable for each cell of time whereby the second computer provides respective values of the second non-predictable code for each of the cells of time for comparison with said first non-predictable code.

According to a second aspect, there is provided a method, wherein the second interval of time comprises a central cell of time and one or more bordering cells of time; using the algorithm of the second computer to calculate independently a plurality of second non-predictable codes on the basis of the static variable and second dynamic variables defined by the cells of time; and determining when a match occurs between the first non-predictable code and one of the second non-predictable codes.

An embodiment of the present invention will now be described, by way of example only, with reference to the accompanying drawings in which:

Figure 1 is a block diagram of a basic apparatus and method according to the invention for generating and comparing non-predictable codes;

Figure 1A is a block diagram of a preferred apparatus and method for generating and comparing non-predictable codes where a means for

comparing non-predictable codes is included in a calculator which generates a non-predictable code;

Figure 2 is a front isometric view of a credit card sized calculator for calculating a first non-preditable code for use in gaining clearance or access according to the invention;

Figure 3 is a flow chart demonstrating a most preferred series of steps carried out by an apparatus according to the invention and/or in a method according to the invention; and

Figures 4 to 9 are diagrammatic representations of series of resultant code cells separately generated by separate computers according to exemplary situations described herein; each diagram sets forth the relationship via a via real time between resultant codes generated on the basis of time as kept by separate clock mechanisms in the separate computers generating the resultant codes according to the corresponding exemplary conditions described with reference to each Figure.

In accordance with the invention an authorised person is provided with a fixed secret code or card seed 10, Figures 1, 1A, 2, 3, typically a number, which is unique to that individual. In the case of a credit or bank/cash card 20, Figure 2, that number 10 may be printed on the card itself such that if the authorised owner of the card forgets the number, it can be quickly retrieved by reference to the card or other permanently printed form of the fixed code 10. Where the fixed code/card seed 10 is provided in permanent printed form on or in close connection with the apparatus of the invention there is also preferably provided an additional portion of the fixed code 10, a so-called pin 45 (personal identification number), which the authorised user memorises in order to further guard against misappropriation of the fixed code/card seed 10. The fixed code/card seed 10 or pin 45 may alternatively be used to identify an authorized terminal which has been issued by the authority presiding over the granting of clearance or access.

Such a fixed and/or memorized code (commonly referred to as a pin 45, FIG. 3, or personal identification number) is input into an access control module ("ACM") or host computer 50, FIGS. 1, 1A, 3 together with the unique static variable 10 and temporarily stored within the memory of the host or ACM, step 100, FIG. 3.

Preferably once the card seed 10 and pin 45 are input into the host or ACM 50, each is separately compared against a library of authorized card pins, step 110, FIG. 3, and a library of authorized card seeds, step 120, FIG. 3, stored in the host or ACM memory to determine whether there is a match. If either of the pin 45 or card seed 10 which the user inputs into the host or ACM does not produce a match, clearance or access is denied and the card user must start over in order to gain access or clearance.

In order to generate a non-predictable code 40, FIGS. 1 - 3, which will ultimately give the user clearance or access, the fixed code or seed 10 and/or pin 45 must be input into a predetermined algorithm which manipulates the seed 10 and/or pin 45 as a static variable. The algorithm is typically provided to the user in the form of a calculator 20, FIG. 2, which is loaded with a program for carrying out the predetermined algorithm. The calculator 20 preferably comprises an electronic computer and most preferably comprises a microprocessor having a sufficient amount of volatile dynamic memory to store and carry out the functions of the predetermined algorithm. The computer 20 is most preferably provided in a card 20, FIG. 2, having the appearance and approximate size of a credit card.

Such credit card sized computer 20, FIG. 2, also preferably includes a conventional liquid crystal display 44 for displaying the ultimate non-predictable code 40 generated by the algorithm (referred to in FIG. 3 as "card resultant code"). The non-predictable code 40 thus generated may be visually observed by the user for eventual input into a host computer or ACM 50, FIGS. 1, 1A. 3. As shown in FIG. 2, the preferred form of card computer 20 has a length L of about 3.3 inches, a width W of about 2.1 inches and a depth D of less than about .07 inches. In addition or as an alternative to providing microprocessor 20 with a liquid crystal display 45 for visual observation of the first non-predictable code 40, computer 20 may include means for machine reading the first non-predictable (or card resultant) code 40 and/or pin 45 to the ACM or host 50, or may include sound producing or other means for personally sensing the first non-predictable code 40.

With reference to FIG. 3, after the card and host pins are compared and found to match, step 110, the card seed 10 is typically compared against a library of card seeds stored in the host or ACM memory in order to determine whether there is a match, step 120, FIG. 3. If the card seed 10 input into the host or ACM 50 does not match up with one of the seeds stored in the host library, access or clearance is denied, "no" step 120, FIG. 3.

For purposes of initial explanation the discussion which follows with reference to FIGS. 1 and 1A assumes an embodiment of the invention whereby a single resultant code 70 is generated by the host or ACM 50. The most preferred embodiment of the invention wherein the clock mechanisms which generate the resultant codes 40 and 70, are synchronized and wherein the host or ACM preferably generates a series of resultant, non-predictable

codes, as opposed to a single code 70, is described hereinafter with reference to FIGS. 4 - 9.

In addition to using the seed 10 and/or pin 45 as static variables the predetermined algorithm is designed to utilize a second variable, a dynamic variable 30,60, FIGS. 1, 1A, to calculate the non-predictable codes 40, 70 which may ultimately give access or clearance 90 to the user. A dynamic variable may comprise any code, typically a number, which is defined and determined by the interval of time in which the card seed 10 and/or pin 45 is put into the algorithm of either the card computer 20 or the host or ACM 50. A dynamic variable is most preferably defined by the date and the minute in which the static variable is input into the predetermined algorithm. A dynamic variable thus defined can be seen to change every minute. The dynamic variable could alternatively be defined according to any interval of time, e.g., 2 minutes, 5 minutes, 1 hour and the like. A dynamic variable thus defined would alternatively change every 1 minute, 2 minutes, 5 minutes, 1 hour or with the passage of any other predetermined interval of time.

With reference to FIG. 1 the most preferred means of establishing such a dynamic variable is via a time keeping means, such as on electronic digital clock, which by conventional means automatically inputs, steps a_1 or c_1, the date and specific interval of time (e.g., 1 minute, 2 minutes, 5 minutes, etc.) into the predetermined algorithm of the card 20 or host or ACM 50 in response to the input, step a or c, of the static variable 10 and/or pin 45. The date and time thus generated by the time keeping means may itself be independently manipulated according to another predetermined algorithm prior to input into the first predetermined algorithm of the dynamic variable. The fact that the dynamic variable 30 or 60 being input into the predetermined algorithm constantly changes in absolute value with passage of successive intervals of time of predetermined duration means that the card code 40 or host or ACM code 70 generated according to the predetermined algorithm is also constantly changing with successive intervals of time and is thereby completely non-predictable.

The non-predictability of the codes 40, 70, FIG. 1, generated in the manner described above may be enhanced by the fact that the predetermined algorithm (together with the static variable 10 and/or pin 45 and dynamic variable 30 input thereinto) are preferably stored in the calculator 20 (and/or host or ACM 50) in volatile dynamic electronic memory which is encapsulated with an energizing means which destroys the algorithm, the card seed 10 , and the dynamic variable 30 (or 60) when the electronic memory is invaded, interrupted or violated in any way. The predetermined algorithm thus stored in such volatile dynamic memory cannot be discovered by a would-be thief because the entire memory including the predetermined algorithm is destroyed upon invasion of the memory.

In a preferred embodiment of the invention therefor the card seed 10 is stored in such volatile dynamic memory and by conventional means is automatically input step a, FIGS. 1, 1A, into the algorithm of the first computer 20 at regular intervals of time. Such automatic inputting of the card seed 10 may thereby work in conjunction with the automatic definition and inputting of the first dynamic variable 30 into the predetermined algorithm of the first computer 20 to effect completely automatic generation of the first non-predictable or resultant code 40 at regular intervals of time.

The invention most preferably contemplates providing authorized personnel with a card computer 20, FIG. 2, only, but not with knowledge of the predetermined algorithm included in the computer 20. Authorized personnel are, therefore, provided with a computer 20 capable of carrying out an algorithm which is unknown to such authorized personnel.

In the most preferred embodiment of the invention where the predetermined algorithm provided to authorized users is stored in a volatile dynamic memory encapsulated with an energizing means which destroys the algorithm upon invasion of the memory, the only means of gaining unauthorized clearance or access is to misappropriate possession of the original computer 20 itself and knowledge of the fixed code/card seed 10 (and knowledge of the card pin 45 if employed in conjunction with the invention).

The algorithm may alternatively be designed to manipulate more than one fixed code and/or more than one dynamic variable. Several means for inputting each fixed code and dynamic variable may be included in the calculator 20 provided to users and in the host or ACM 50, FIG. 3. Each dynamic variable is preferably defined by the interval of time in which one or more of the fixed codes/card seeds are input into the algorithm.

It can be seen, therefore, that the predetermined algorithm can comprise any one of an infinite variety of algorithms. The only specific requirement for an algorithm to be suitable for use in the present invention is that such algorithm generate a non-predictable code on the basis of two classes of variables, static variables (the fixed codes) and dynamic variables such as described hereinabove. A non-predictable code C which is ultimately generated by the predetermined algorithm, f (x,y), may be expressed mathematically as:

$$f(x,y) = C$$

where x is a static variable fixed code and y is a dynamic variable. Where several (n) static variables (x_1, x_2, ...x_n) and several (n) dynamic variables (y_1, y_2, ...y_n) are intended for use in generating non-predictable codes, a non-predictable code thus generated may be expressed mathematically as f-(x_1, x_2, ...x_n, y_1, y_2, ...y_n) = C.

The specific form of the algorithm only assumes special importance as part of the invention, therefore, when the algorithm is capable of being discovered by would-be unauthorized users. In the most preferred embodiment of the invention where the algorithm is completely undiscoverable by virtue of its storage in a volatile dynamic electronic memory which destroys the algorithm upon attempted invasion of the encapsulated memory, the specific form of the algorithm comprises only an incidental part of the invention. The mere fact of the use of some algorithm to manipulate the fixed code and the dynamic variable does, however, comprise a necessary part of the invention insofar as such an algorithm generates the ultimately important non-predictable code.

As the term "fixed code" or "card seed" or "seed" is used herein such terms include within their meaning numbers, codes, or the like which are themselves manipulated or changed, mathematically or otherwise, in some non-dynamic manner prior to or during the generation of a second non-predictable code 40, FIG. 3. The first 20 or second computer 50 may, for example, be provided with a static program/algorithm utilizing the fixed code or seed as a variable and generating a new fixed code or seed which is ultimately input as the fixed code or seed 10 variable in the secret algorithm which generates the non-predictable codes. for example, for purposes of added security, a fixed code or seed 10 may be first added to another number and the result thereof used as the fixed code or seed 10 used to generate the non-predictable codes. Thus, the term fixed code or seed includes within its meaning the result of any non-dynamic operation performed on any fixed code or seed. It can be seen, therefore, that essentially any algorithm or operation may be performed on the fixed code 10 to generate another fixed code or seed, the algorithm or operation most preferably comprising a static algorithm or operation, i.e., one not utilizing dynamic variables so as to generate a static result.

With reference to FIG. 1, after a first non-predictable code 40 is generated as described above, such first non-predictable code 40 is compared 80 with the "second" non-predictable code 70 which is also generated by the user by putting, step c, the fixed code/card seed 10 (and the pin 45, if employed) into the host or ACM 50 which contains the same predetermined algorithm used to generate the first non-predictable code 40.

With reference to FIG. 1A, (a schematic diagram which assumes the host or ACM 50 includes the predetermined algorithm and the mechanism for comparing and matching the non-predictable codes) the first non-predictable code 40 is put, step e_2, into the host or ACM 50 essentially immediately after the fixed secret code 10 is put into the host or ACM 50 (i.e., step e_2 is carried out essentially immediately after step e) in order to gain clearance or access 90. If steps e and e_2 are not carried out within the same interval of time as steps a and a_1, were carried out, (i.e., the same interval of time on which code 40 is based), then the host or ACM will not generate a second dynamic variable 60 which will allow the predetermined algorithm of the host or ACM 50 to generate a second non-predictable code which matches the 1st non-predictable code 40.

The necessity for carrying out steps e and e_2, FIG. 1A, within the same minute or other selected interval of time ("cell") is obviated in a most preferred embodiment of the invention. With reference to FIGS. 3 - 4, the card 20 generates a resultant code 40, on the basis of a cell of time in which the code 40 was generated as defined by the card clock. Assuming for the sake of explanation that the card clock and the host or ACM clock 125 are synchronized with each other and with real time and assuming the user inputs the correct card seed 10 and resultant code 40 into the host or ACM 50 within the same cell of time as the resultant code 40 was generated by the card 20 the host 50 is preferably provided with a program which generates a series or "window" of resultant codes (as opposed to a single non-predictable code 70, FIG. 1). [As used hereinafter, the term "cell" is, depending on the context, intended to refer to an interval of time of predetermined duration on which the generation of a resultant code is based or to the resultant code itself.] The various second non-predictable codes which comprise the "window" are calculated by the host or ACM 50 on the basis of the cell of time in which the user correctly entered the seed 10, code 40, and pin 45 into the host or ACM 50 as defined by the host clock 125, FIG. 3, and one or more bordering cells of time, e.g., -2, -1, and +1, +2 as shown in FIG. 4. An ACM or host computer 50 program then compares the card resultant code 40 with all of the individual resultant codes computed as the window of host cells shown in FIG. 4 to determine whether there is a match between any of the host cells and the card code 40. In the example stated, the card code 40 will of course match up, step 172, FIG. 3, with the zero cell-based host code, FIG. 4 because the user input the seed 10, pin 45 and code 40 within the same cell of time as the card code 40 was gen-

erated.

[As used hereinafter, "input" or "inputting" or "entry" into the host or ACM 50 refers to input of the correct card seed 10, card resultant code 40 and card pin 45 into the host or ACM 50 and positive matching of the card seed 10, step 120, FIG. 3, and card pin 45, step 110, with a host seed and host pin which are stored in the permanent memory in the host or ACM 50].

Assuming in the example stated above with reference to FIG. 4, however, that the user had input the card code 40 and seed 10 (and pin 45), FIG. 3, one minute later than the card had generated the code 40, the host or ACM 50 will have generated a different window of codes as shown in FIG. 5; that is, the host will have generated a central cell correspoding to a +1 cell code (based on real time) as if the +1 cell code is the zero cell of the window of cell (as shown in parenthesis in FIG. 5) and further generate the predetermined number of bordering cell codes (e.g., real time -1,0 and +2, +3 as shown in FIG. 5). Thus although the user inputs the card seed 10 and the card resultant code 40 into the host or ACM 50 one minute late, the host computer 50 still generates a matching cell code, the real time zero cell code which "borders" the central cell, i.e., the +1 central cell code as shown in parenthesis in, FIG. 5.

Provision of the host or ACM 50, FIGS. 3 - 5 with a mechanism for generating a series or window of second non-predictable codes, as opposed to a single second code 70, FIG. 1, thereby allows a card user a selected amount of leeway of time (beyond the time length of the interval of time on which code 40 is based) in which to input a correct seed 10, pin 45 and card code 40 into the host or ACM 50 and still generate a matching host resultant code.

The examples stated above assumed that the card clock and the host clock 125, FIG. 3 were both synchronized with real time. Assuming the card clock and the host clock remain synchronized at all times, it would only be necessary to provide the host or ACM 50 with a mechanism for generating a selected number of bordering cells which "precede" the central cell of the window, e.g., with reference to FIG. 5, the (-2), (-1), (0) cells. In those applications where the card clock and the host clock are maintained in synchrony with each other at all times, the host or ACM clock 125 preferably defines only two dynamic time variables so as to generate a central cell code and a -1 host window cell code. Such embodiment allows the user to input to seed 10, pin 45 and code 40 one cell code late but only one cell code late for security enhancement.

In the more typical case, however, where the card clock and the host clock 125 may be out of synchrony with real time, e.g., where the card clock is running fast relative to the host clock, the generation of cells which "follow" the central cell of the host window may be required to generate a matching host resultant code.

With reference to FIG. 3, 6 the invention most preferably provides a mechanism for synchronizing the card and host clocks in the case where such independent clocks more typically run fast or slow relative to real time and/or relative to each other.

The following examples assume for purposes of explanation that the time equivalent length of all cell codes are one minute in duration. Assuming that the card clock is one minute slow and the host clock 125, FIG. 3 is correct relative to real time, the card will generate a resultant code 40 based on a real time of -1 minute (relative to the host clock 125) and, if the user inputs the card resultant code 40 (and the correct seed 10 and pin 45) into the host or ACM 50 within the same minute as the code 40 is generated, the host or ACM 50 will generate a window of resultant codes according to the series of cells shown in FIG. 6 (assuming the predetermined number of bordering cells is selected as 2 cells immediately preceding and 2 cells immediately following). Matching resultant codes, i.e., the card -1 cell code and the host -1 cell code, will thus have been generated.

Although the card clock was one minute slow in the example just described, the host computer is provided with a program mechanism which will automatically adjust (i.e., synchronize) the host clock time with the card clock time when the card user next enters a correct card seed 10 and card pin 45 (and code 40) into the host or ACM 50. The host accomplishes such synchronization by storing a difference in matching cell time in the permanent memory of the host, step 190, FIG. 3; e.g., in the example just described, the last matching transaction, step 180, FIG. 3 fell in the -1 cell of the host "window" as shown in parenthesis in FIG. 6. Such cell time difference is referred to herein as the "time offset" which is stored in the permanent host memory, step 190, FIG. 3. The time offset is the difference in time between the central cell and the bordering cell from which a matching second non-predictable code was generated.

Upon the next entry of the card user into the host 50 (assuming the card clock has not run any slower since the last entry and assuming the host clock has remained synchronized with real time and assuming the user next enters the host 50 within the same minute as the card generates resultant code 40), the host computer 50 will automatically algebraically add the stored time offset, steps 135, 140, FIG. 3, to the temporarily stored host clock time, step 130, and generate the series of relative real time host cell codes shown in FIG. 7

wherein the card code cell which is one minute slow in real time, is now treated in the host window as a zero cell (as shown in parenthesis in FIG. 7), i.e., the central cell of the host window of cells, is adjusted to subtract one minute therefrom, via subtraction of the one-minute stored time offset 135, FIG. 3. As shown in FIG. 7, the bordering cells of the host window are similarly adjusted by the one-minute stored time offset. Further, in all future entries by the user into the host 50, the temporarily stored time and date of entry, step 130, FIG. 3, will be adjusted by the permanently recorded one-minute stored time offset.

As to the example described above with reference to FIG. 5 wherein the card and host clocks were assumed to be synchronized with real time and wherein the user entered the host one minute late, it is noted that even though the host clock was synchronized with real time, the host will nevertheless compute a time offset, step 180, FIG. 3, to be stored, step 190, and used in adjusting the temporarily stored time of entry, step 130, FIG. 3, in future transactions by the user, because the matching cell of the host window, as shown in parenthesis FIG. 5, was not the central cell code of the window (i.e., was not the real time +1 cell code) but rather was a bordering real time cell code, i.e., the bordering real time zero cell code.

Simply stated, therefore, a stored time offset will be computed step 180, FIG. 3, and stored, step 190, FIG. 3, for use in adjusting the time of entry into the host in all future entries, step 140, FIG. 3, whenever on a given entry, step 130, FIG., 3, a "bordering" cell code of the host window (as opposed to the central cell code) produces a match with the input card resultant code 40.

In storing, step 190, FIG. 3, a time offset which is computed, step 180, during any given transaction, the presently computed time offset is algebraically added or summed to any time offsets previously computed and stored as a result of previous entries and grantings of access, step 173.

Inasmuch as a clock mechanism, once beginning to run fast or slow, will continue to run fast or slow during all future uses of the system of the invention, the host or ACM 50 will add or subtract all time offsets recorded during successive uses of the system to the stored time offset(s) recorded and permanently stored from previous transactions, step 180, FIG. 3. Most preferably, a newly computed time offset will not be permanently stored, step 190, in the host or ACM memory 200, unless and until access or clearance has already been granted, step 173.

As described and shown in the examples of FIGS. 4 - 7 the host or ACM is typically programmed to compute four (4) cell codes bordering the central cell code (i.e., two cells immediately preceding and two cells immediately following the central cell) as the "window" within which the user is allowed to deviate in inputting the card seed 10, the pin 45, and, the card resultant code 40 into the host or ACM. Such bordering cells have been described as corresponding to codes corresponding to one-minute intervals. It is noted that the number and time equivalent length of the bordering cells may be increased or decreased as desired.

The absolute degree by which the card clock and the host or ACM clock 125 may run fast or slow relative to real time typically increases with the passage of time. For example, if the card clock is running slow by 30 seconds per month and the host clock is running fast at 30 seconds per month, the two clocks will run the time equivalent of one minute out of synchrony after one month, two minutes out of synchrony after two months, three minutes out of synchrony after three months, etc. If the authorized card user uses the card each month, the automatic synchronizing means described above with reference to FIGS. 4 - 7 will have adjusted the host or ACM time window upon each usage to account for such lack of synchrony with real time. If, however, the card user does not actually use the card for, for example, six months, the card clock and the host clock will be six minutes out of synchrony, and even if the user correctly uses the system by inputting the pin 45, card seed 10 and card code 40, FIG. 3, into the host or ACM within the same minute (or other selected time cell interval) as the pin 45, the seed 10 and code 40 were generated by the card, the user would not be able to gain access or clearance (i.e., cause the host or ACM to generate a matching resultant code) in the typical situation where the "window" of bordering cell times is selected as two one-minute cells immediately preceding and two one-miniute cells immediately following the central host cell. FIG. 8 depicts such an exemplary situation as just described, wherein it can be seen that the card clock, after six months of non-usage, generates a resultant code 40, FIG. 3, which is based on -3 minutes in real time, and the host clock, after six months of non-usage, causes the generation of the typically selected five cell window comprising cell codes corresponding to +1, +2, +3, +4, and +5 minutes in relative real time. In the typical case, therefore, where the selected window comprises four bordering cells, matching second non-predictable codes will not be generated under any circumstances after six months of non-use.

The invention most preferably provides a mechanism by which the host window of bordering cells is opened wider than the preselected window by an amount which varies with the length of time of non-use of the card. Such window opening is accomplished by storing the most recent date of

comparison and matching, determing the difference in time between such date and the present date of entry into the second computer and calculating as many additional bordering cells as may be predetermined according to the difference in time between the dates.

Typically the window is opened by two one minute bordering cells per month of non-use (e.g., one cell immediately preceding and one cell immediately following the preselected window) but the number of cells by which the window is opened and the time equivalent length of each cell may be predetermined to comprise any other desired number and length.

Assuming the exemplary situation described above where the card clock and the host clock 125, FIG. 3, are running slow and fast respectively by 30 seconds per month and the user has not used the card for six months, the host or ACM compares, step 150, the temporarily stored date of the present entry, step 130, with the permanently stored date of the last access, step 175, and computes the number of months X, step 160, between the date of last access and the date of present entry. In the present example six months of non-use is calculated step 160, FIG. 3, and the window is opened by six additional one-minute bordering cells on either side of the preselected four cell window as shown in FIG. 9 to give an overall window of sixteen minutes. The card resultant code 40 based on -3 minutes in relative real time thus matches, step 172, FIG. 3A, as shown in FIG. 9 with the -6 host bordering cell code (-3 in real time) and access or clearance is ultimately granted. As described above with reference to FIGS. 4 - 7, because the matching host cell code is a bordering cell code of the host window and not the central host cell (i.e., the zero cell), a new stored time offset of -6 minutes will be computed (i.e., added to the permanently stored time offset), step 180, FIG. 3, and stored, step 190, and the host clock thereafter will adjust the zero cell of the host window (and accompanying bordering cells) each time the user of the card having the particular card seed 10 and pin 45 which was used in the present transaction uses the card to gain access in future transactions.

Lastly the invention further includes a failsafe window opening mechanism to provide for the contingency where the host or ACM 50 and its clock 125, FIG. 3, may shut down between card usages. In the event of such a shut down, the host or ACM clock 125 must typically be reset and re-synchronized, and in the course of such re-setting an error may be made in the resynchronization. In order to insure that the card user may reasonably gain access in the event of such an error in re-setting the host clock 125, the host or ACM 50 is preferably provided with a mechanism for sensing such a re-setting and for storing a predetermined window opening number upon each re-setting of the host or ACM 125. Such window opening number is typically selected as six additional one-minute bordering cells (e.g., three additional cells immediately preceding and three additional cells immediately following the existing window) but may be selected as more or fewer cells of other selected length.

The re-setting window opening number is typically added, step 165, FIG. 3, to the result of non-usage step 160 and the total additional number of cells comprising the window is computed, step 170, FIG. 3, i.e., all bordering cells surrounding the central cell are computed including (a) the preselected window allowing for user delay in inputting and/or card and host clock asynchrony, (b) the no-usage window allowing for card and host clock asynchrony over long periods of time of non-usage and (c) the re-setting window opening number.

Assuming the exemplary situation described above with reference to FIG. 9, if the host or ACM had shut down within the six month period of non-use, the host window as depicted in FIG. 9 would be further opened by an additional six bordering cells such that -11, -10, -9 and +9, +10, +11 host window cells would also have been computed, step 170, FIG. 3, and made available for comparison and potential matching with card resultant code 40 in step 172, FIG. 3. As described with reference to FIGS. 5 - 9, where a new time offset is computed and stored, steps 180, 190, FIG. 3, as a result of a match found in a bordering cell of a window generated by virtue of non-usage and/or the preselected window, a new time offset will similarly be computed and stored, steps 180, 190, if a match is found in a bordering cell generated as a result of shut-down.

Unlike the non-usage window opening number, the re-set window opening number is typically stored in the permanent memory 200 of the host or ACM 50, FIG. 3, such that once the host clock 125 is re-set, the selected window opening number is available in permanent memory 200 to open the window upon the next attempted entry by the user. Although the re-set window opening number is established and stored in permanent memory 200, such re-set window opening number is preferably eventually closed down or eliminated for security enhancement after it is established upon successive attempted entries by a variety of card users that the host clock 125 was correctly reset or after the host clock 125 is otherwise re-synchronized with real time to correct any errors which may have occurred as a result of the re-setting. The use of the re-set window opening number is, therefore, preferably temporary.

In the practical application of the invention, many cards are issued to many users and each card includes its own card clock. Recognizing that the average of the times being kept by the individual clocks of a statistically significant sample of a variety of cards, will produce an accurate or very nearly accurate representation of real time, the invention most preferably includes a mechanism for permanently adjusting the time kept by the host clock 125, FIG. 3, after the clock 125 has been re-set, to the average of the times of entry (after re-setting of the host clock 125) of a selected number of different cards or card users. For example, assuming that host clock 125 has been reset, the next time of entry of the next five (or other selected number of) separate card users is averaged, the host clock 125 is permanently adjusted or re-synchronized to such an averaged time, and the re-set window opening number is thereafter eliminated from the permanent host memory 200. Re-adjusting or re-synchronization of the host clock 125 to the averaged time of the card clocks is typically carried out by the host 50 by computing another master time offset which is algebraically added to the time offsets peculiar to each card 20. The computation of such a master offset assumes that a selected number of separate cards 20 were able to gain access, step 173, FIG. 3 as a result of the re-set window opening or otherwise. The average of the time offsets computed as to the selected number of cards which enter the host 50 (after the host clock 125 is re-set) is preferably stored as a master time offset (i.e., as a re-synchronization of the host clock 125), the re-set window opening number is then eliminated as to all future entries by card users, and the master time offset is used (in addition to permanently stored time offsets peculiar to each card) to adjust the card clock 125 in transactions as to all card entries thereafter.

As a practical matter, a limit is typically placed on the total number of bordering cells by which the window is opened regardless of the length of time of non-usage by the card user or the number of times the host or ACM 50 is reset as a result of re-setting of clock 125. For security reasons, such a limit is typically selected as ten one-minute bordering cells - as stated in step 170, FIG. 3 the number of codes comprising the window are the lesser of (a) 4 bordering cell codes, the preferred selected window, plus X, the number of months or other selected non-usage periods, plus Y, the shut down window opening number, or (b) 10, the maximum number of additional cell codes. Such a maximum window may, of course, be selected as more or less than 10 depending on the degree of security desired.

It is noted that FIG. 3 depicts a preferred sequence of operations and not necessarily the only sequence. Steps 110 and 100 could, for example, be interchanged or, for example, the step of automatically inputting the re-set window opening number, step 167 could precede any of steps 140 - 160.

The host or ACM 50, FIGS. 1, 1A, 3' typically includes one or more programs and sufficient memory to carry out all of the steps shown in FIG. 3, although one or more of those functions may be carried out by a device separate from and communicating with or connected to the host or ACM 50.

With respect to the computation, storage and retrieval of time offsets, the host or ACM 50 is provided with mechanisms for recognizing, storing, retrieving and computing time offsets which are peculiar to each card seed 10 and/or pin 45 and responsive to the input of the same into the host or ACM 50.

FIG. 2 depicts the most preferred form of the calculator 20 which is provided to authorized users for generating the first non-predictable or card resultant code 40. As shown in FIG. 2 the calculator 20 is of substantially the same size as a conventional credit card and includes a conventional liquid crystal display 44 for displaying the code 40 to the user. The credit/card computer 20, FIG. 2, may bear the identity of the card seed/fixed code 10 printed on its face, and includes a digital clock means, an energizing means, a microprocessor and sufficient memory for storing the predetermined secret algorithm, a program for generating a dynamic variable if desired, and the card seed 10 and pin 45 if desired.

In an embodiment of the invention where the goal is to grant access to a physical facility, the ACM 50 may comprise a portable device such that it may be carried by a security guard stationed at a central access location leading to a guarded building or other facility. A security guard thus in possession of such an ACM would typically read the card seed 10 and the non-predictable code 40 appearing on the card 20, FIG. 2, of authorized person and input such codes 10, 40 (in addition to the pin 45 – otherwise provided to the guard by the card bearer) into the portable ACM 50 to determine whether the card bearer is truly in possession of a card 20 which was issued by the authority establishing the secret predetermined algorithm.

As described herein protection of the secrecy of the predetermined algorithm is preferably accomplished in the calculators provided to authorized personnel by virtue of its storage in volatile dynamic memory and encapsulation with a volatile dynamic energizing means. With respect to the algorithm provided in the ACM secrecy may be maintained in a similar manner or other conventional manner, e.g., by physically guarding the ACM or requiring additional access/user codes to

gain direct access. Where all programs, data and results of operation are stored in such volatile dynamic memory, the same are similarly protected against invasion.

Although the invention contemplates some form of communication of the result of operation 40 carried out on the card 20, FIG. 2, to the host or ACM 50 or any other electronic device, a talking between the computer 20 and the host 50 is not required or contemplated by the invention. Therefore, after the first computer 20 has calculated the first non-predictable code 40 and the code 40 has been input into the host 50, no other information need be communicated back to the first computer 20 from the host 50 or another device in order to gain clearance or access.

Lastly it is noted that the fixed code or seed 10 and/or pin 45, FIG. 3, may be employed to identify a computer terminal or other piece of equipment or device as opposed to a card 20. For example, a terminal or a space satellite or other device may be provided with a computer 20 which is assigned a code or seed 10 and/or a pin 45 (and, of course, provided with the secret predetermined algorithm and a clock and conventional electronic mechanisms for computing the code 40 and inputting the code 10, pin 45, and resultant code 40 to the host or ACM 50) in order to identify such terminal, satellite or the like in the same manner as a card computer 20 is identifiable as described hereinabove.

Claims

1. A system for comparing and matching non-predictable codes generated by separate computers, comprising:
a first computer (20), operable to produce a first non-predictable code (40) on the basis of a first dynamic variable (30) and a static variable (10), a first clock means for defining the first dynamic variable (30), according to a first interval of time during which the static variable is input into the first computer (20),
a second computer (50), operable to produce a second non-predictable code (70) on the basis of a second dynamic variable (60) and the static variable (10), a second clock means for defining the second dynamic variable (60), according to a second interval of time during which the static variable (10) is input into the second computer (50), and
means (80) for comparing the first and second non-predictable codes (40, 70) to determine a match,
characterised in that
the second interval of time comprises a central cell of time, having a predetermined duration, and one or more cells of time, each having a predetermined duration, bordering the central cell, and **in that**
the second clock means defines respective values of the second dynamic variable (60) for each cell of time whereby the second computer provides respective values of the second non-predictable code for each of the cells of time for comparison with said first non-predictable code.

2. A system according to claim 1 wherein there is provided means for synchronising the first clock means and the second clock means upon matching of the first non-predictable code (40) with one of the second non-predictable codes (70).

3. A system according to claim 1 or 2 wherein the central cell of time comprises the date and the minute in which the unique static variable is input into the second computer (50) as defined by the second clock means.

4. A system according to claim 1, 2 or 3 wherein the bordering cells of time comprise a cell of time comprising the date and the minute immediately preceding the central cell.

5. A system according to any preceding claim wherein the border cells of time comprise a selected number of cells of time immediately preceding the central cell and a selected number of cells of time immediately following the central cell.

6. A system according to any preceding claim wherein the central and border cells of time are selected to be one minute in duration.

7. A system according to any of claims 2 to 6 including:
counting means for counting the difference in time between a central cell of time and a bordering cell of time from which a matching second non-predictable code (70) may be generated;
summing means connected to the counting means for summing successive differences in time counted by the counting means;
storage means connected to the summing means for storing the output of the summing means; and
shifting means connected to the storage means for shifting a central cell and bordering cells of time by the summed times stored in the storage means.

8. A system according to claim 7 including:
second storage means connected to the comparison means for storing the date of the most recent comparison and matching by the comparison means;
second counting means connected to the second storage means for counting the difference in time between the date stored and the date of present entry into the second computer;
dividing means connected to the second counting means for dividing the difference in time counted by the second counting means by a selected value and prescribing the output as a first window opening number;
window opening means connected to the dividing means and the comparison means for calculating as many extra second non-predictable codes on the basis of as many extra bordering cells of time immediately preceding and following the selected number of border cells as prescribed by the first window opening number.

9. A system according to claim 8 further including:
sensing means connected to the second clock means for sensing a re-setting of the second clock means;
third storage means connected to the sensing means for prescribing and storing the occurrence of a sensed re-setting of the second clock means as a selected second window opening number; and
second window opening means connected to the third storage means for calculating as many additional non-predictable codes on the basis of as many additional bordering cells of time immediately preceding and following the extra border cells of time as prescribed by the second window opening number.

10. A system according to any preceding claim wherein the first or the second computer (20, 50) comprises a microprocessor with an algorithm stored in volatile dynamic memory with an energizing means that when interrupted destroys all data including at least the algorithm and the static variable.

11. A system according to any preceding claim wherein the first computer (20) and the first clock means are incorporated into a card of about the same size as a credit card.

12. A system according to any preceding claim wherein said first computer (50) includes means (44) for visually displaying the non-predictable code (40) currently being generated.

13. A system as claimed in claim 10 wherein said card has a length of approximately 84mm (3.3 inches), a width of approximately 53mm (2.1 inches), and a depth approximately 1.8mm (.07 inches).

14. A system as claimed in claim 12 wherein said usual display means (44) is a liquid crystal display.

15. A method of synchronising the time definition of dynamic variables (30, 60) in a system for comparing non-predictable codes (40, 70) generated by separate clock means according to time wherein the codes match when the dynamic variables match, comprising the steps of:
inputting a static variable (10) into a first computer (20) including a predetermined algorithm;
employing the algorithm of the first computer (20) to calculate a first non-predictable code (40) on the basis of the static variable (10) and a first dynamic variable (30) defined by a first interval of time in which the step of inputting occurred according to a first clock;
independently feeding the static variable (10) and the first non- predictable code (40) into a second computer (50) including the predetermined algorithm;
using the algorithm of the second computer (50) to independently calculate a second non-predictable code (70) on the basis of the static variable (10) and a second dynamic variable (60) defined by a second interval of time in which the step of feeding occurred according to a second clock means; and
comparing the first and second non-predictable codes (40, 70) to determine a match;
characterised in that:
the second interval of time comprises a central cell of time and one or more bordering cells of time; **and by:**
using the algorithm of the second computer (50) to calculate independently a plurality of second non-predictable codes (70) on the basis of the static variable (10) and second dynamic variables (60) defined by the cells of time; and
determining when a match occurs between the first non-predictable code (40) and one of the second non-predictable codes (50).

16. The method according to claim 15 further including the steps of:
counting the difference in time between a central cell of time and a bordering cell of time

from which a matching second non-predictable code may be generated; summing successive differences in time counted during the step of counting;
storing the summed successive differences in time; and,
shifting the central and border cells of time by the summed successive differences in time.

17. The method according to claim 16 further including the steps of:
storing the date of the most recent comparison and determination of a match;
counting the difference in time between the date stored and the date of present entry into the second computer;
diving the difference counted during the step of counting the difference in dates by a selected value and prescribing the output as a first window opening number; and,
calculating as many extra second non-predictable codes (70) on the basis of as many extra bordering cells of time immediately preceding and following the selected number of border cells as prescribed by the first window opening number.

18. The method according to claim 17 including the steps of:
sensing a re-setting of the second clock means;
prescribing and storing the occurrence of a sensed re-setting of the second clock means as a second selected window opening number; and,
calculating as many additional second non-predictable codes (70) on the basis of as many additional border cells of time immediately preceding and following the extra border cells of time as prescribed by the second window opening number.

19. The method of claim 15 wherein the central and bordering cells of time are selected to be one minute in duration.

Revendications

1. Système destiné à comparer et accorder des codes non prévisibles générés par des calculateurs séparés, comportant :
un premier calculateur (20) utilisable pour produire un premier code non prévisible (40) sur la base d'une première variable dynamique (30) et d'une variable statique (10), un premier moyen d'horloge destiné à définir la première variable dynamique (30) conformément à un premier intervalle de temps pendant lequel la variable statique est introduite dans le premier calculateur (20),
un second calculateur (50) utilisable pour produire un second code non prévisible (70) sur la base d'une seconde variable dynamique (60) et de la variable statique (10), un second moyen d'horloge destiné à définir la seconde variable dynamique (60) conformément à un second intervalle de temps pendant lequel la variable statique (10) est introduite dans le second calculateur (50), et
un moyen (80) destiné à comparer les premier et second codes non prévisibles (40, 70) pour déterminer un accord,
caractérisé en ce que
le second intervalle de temps comprend une cellule centrale de temps ayant une durée prédéterminée, et une ou plusieurs cellules de temps ayant chacune une durée prédéterminée, bordant la cellule centrale, et en ce que
le second moyen d'horloge définit les valeurs respectives de la seconde variable dynamique (60) pour chaque cellule de temps afin que le second calculateur produise des valeurs respectives du second code non prévisible pour chacune des cellules de temps pour une comparaison avec ledit premier code non prévisible.

2. Système selon la revendication 1, dans lequel il est prévu des moyens destinés à synchroniser le premier moyen d'horloge et le second moyen d'horloge à la suite d'un accord du premier code non prévisible (40) avec l'un des seconds codes non prévisibles (70).

3. Système selon la revendication 1 ou 2, dans lequel la cellule centrale de temps comprend la date et la minute dans laquelle la variable statique unique est introduite dans le second calculateur (50) comme défini par le second moyen d'horloge.

4. Système selon la revendication 1, 2 ou 3, dans lequel les cellules de temps bordantes comprennent une cellule de temps comprenant la date et la minute précédant immédiatement la cellule centrale.

5. Système selon l'une quelconque des revendications précédentes, dans lequel les cellules de temps bordantes comprennent un nombre choisi de cellules de temps précédant immédiatement la cellule centrale et un nombre choisi de cellules de temps suivant immédiatement la cellule centrale.

6. Système selon l'une quelconque des revendi-

cations précédentes, dans lequel les cellules de temps centrale et bordantes sont choisies de façon à avoir une durée d'une minute.

7. Système selon l'une quelconque des revendications 2 à 6, comprenant :

un moyen de comptage destiné à compter la différence de temps entre une cellule centrale de temps et une cellule bordante de temps à partir de laquelle un second code non prévisible adapté (70) peut être généré ;

un moyen de sommation connecté au moyen de comptage pour établir une somme de différences de temps successives comptées par le moyen de comptage ;

un moyen de stockage connecté au moyen de sommation pour stocker les signaux de sortie du moyen de sommation ; et

un moyen de décalage connecté au moyen de stockage pour décaler une cellule centrale et des cellules bordantes de temps des temps obtenus par sommation et stockés dans le moyen de stockage.

8. Système selon la revendication 7, comprenant :

un second moyen de stockage connecté au moyen de comparaison et destiné à stocker la date de la comparaison la plus récente et de l'adaptation établie par le moyen de comparaison ; un second moyen de comptage connecté au second moyen de stockage et destiné à compter la différence de temps entre la date stockée et la date de l'entrée présente dans le second calculateur ;

un moyen de division connecté au second moyen de comptage et destiné à diviser la différence de temps comptée par le second moyen de comptage par une valeur choisie et à prescrire le signal de sortie en tant que premier numéro d'ouverture d'une fenêtre ;

un moyen d'ouverture de fenêtre connecté au moyen de division et au moyen de comparaison pour calculer autant de seconds codes non prévisibles supplémentaires sur la base d'autant de cellules de temps bordantes supplémentaires précédant et suivant immédiatement le nombre choisi de cellules bordantes que prescrit par le premier numéro d'ouverture de fenêtre.

9. Système selon la revendication 8, comprenant en outre :

un moyen de détection connecté au second moyen d'horloge pour détecter une remise à l'état initial du second moyen d'horloge ;

un troisième moyen de stockage connecté au moyen de détection pour prescrire et stocker l'apparition d'une remise à l'état initial détectée du second moyen d'horloge en tant que second numéro choisi d'ouverture d'une fenêtre ; et

un second moyen d'ouverture de fenêtre connecté au troisième moyen de stockage pour calculer autant de codes non prévisibles additionnels sur la base d'autant de cellules de temps bordantes additionnelles précédant et suivant immédiatement les cellules de temps bordantes supplémentaires que prescrit par le second numéro d'ouverture de fenêtre.

10. Système selon l'une quelconque des revendications précédentes, dans lequel le premier ou le second calculateur (20, 50) comporte un micro-processeur pourvu d'un algorithme stocké dans une mémoire dynamique volatile avec un moyen d'excitation qui, lorsqu'il est interrompu, détruit toutes les données comprenant au moins l'algorithme et la variable statique.

11. Système selon l'une quelconque des revendications précédentes, dans lequel le premier calculateur (20) et le premier moyen d'horloge sont incorporés dans une carte ayant sensiblement les mêmes dimensions qu'une carte de crédit.

12. Système selon l'une quelconque des revendications précédentes, dans lequel ledit premier calculateur (50) comprend un moyen (44) destiné à afficher de façon visuelle le code non prévisible (40) en cours de génération.

13. Système selon la revendication 10, dans lequel ladite carte a une longueur d'environ 84 mm (3,3 inches), une largeur d'environ 53 mm (2,1 inches) et une profondeur d'environ 1,8 mm (0,07 inch).

14. Système selon la revendication 12, dans lequel ledit moyen d'affichage habituel (44) est un visuel à cristaux liquides.

15. Procédé de synchronisation de la définition dans le temps de variables dynamiques (30, 60) dans un système destiné à comparer des codes non prévisibles (40, 70) générés par des moyens d'horloge séparés en fonction du temps, dans lequel les codes s'accordent lorsque les variables dynamiques s'accordent, comprenant les étapes qui consistent :

à introduire une variable statique (10) dans un premier calculateur (20) comprenant un algorithme prédéterminé ;

à utiliser l'algorithme du premier calculateur (20) pour calculer un premier code non

prévisible (40) sur la base de la variable statique (10) et d'une première variable dynamique (30) définie par un premier intervalle de temps dans lequel l'étape d'introduction a eu lieu conformément à une première horloge ;

à procéder à une entrée indépendante de la variable statique (10) et du premier code non prévisible (40) dans un second calculateur (50) comprenant l'algorithme prédéterminé ;

à utiliser l'algorithme du second calculateur (50) pour calculer de façon indépendante un second code non prévisible (70) sur la base de la variable statique (10) et d'une seconde variable dynamique (60) définie par un second intervalle de temps dans lequel l'étape d'entrée a eu lieu conformément à un second moyen d'horloge ; et

à comparer les premier et second codes non prévisibles (40, 70) pour déterminer un accord ;

caractérisé en ce que :

le second intervalle de temps comprend une cellule centrale de temps et une ou plusieurs cellules de temps bordantes ;

et en ce qu'il consiste :

à utiliser l'algorithme du second calculateur (50) pour calculer de façon indépendante plusieurs seconds codes non prévisibles (70) sur la base de la variable statique (10) et de secondes variables dynamiques (60) définies par les cellules de temps ; et

à déterminer lorsqu'un accord apparaît entre le premier code non prévisible (40) et l'un des seconds codes non prévisibles (50).

16. Procédé selon la revendication 15, comprenant en outre les étapes qui consistent :

à compter la différence de temps entre une cellule centrale de temps et une cellule bordante de temps à partir de laquelle un second code non prévisible adapté peut être généré ;

à établir la somme de différences successives de temps comptées durant l'étape de comptage ;

à stocker les différences successives de temps dont la somme est réalisée : et

à décaler les cellules de temps centrale et bordantes de la somme des différences de temps successives.

17. Procédé selon la revendication 16, comprenant en outre les étapes qui consistent :

à stocker la date de la comparaison et de la détermination d'un accord les plus récentes ;

à compter la différence de temps entre la date stockée et la date d'entrée présente dans le second calculateur ;

à diviser la différence comptée durant l'étape de comptage de la différence de date par une valeur choisie et à prescrire le signal de sortie en tant que premier nombre d'ouverture d'une fenêtre ; et

à calculer autant de second codes non prévisibles supplémentaires (70), sur la base d'autant de cellules de temps bordantes supplémentaires précédant et suivant immédiatement le nombre choisi de cellules bordantes, que prescrit par le premier numéro d'ouverture de fenêtre.

18. Procédé selon la revendication 17, comprenant les étapes qui consistent :

à détecter une remise à l'état initial du second moyen d'horloge ;

à prescrire et stocker l'apparition d'une remise à l'état initial détectée du second moyen d'horloge en tant que second numéro choisi d'ouverture de fenêtre ; et

à calculer autant de seconds codes non prévisibles additionnels (70) sur la base d'autant de cellules de temps bordantes additionnelles précédant et suivant immédiatement les cellules de temps bordantes supplémentaires que prescrit par le second numéro d'ouverture de fenêtre.

19. Procédé selon la revendication 15, dans lequel les cellules de temps centrale et bordantes sont choisies de façon à avoir une durée d'une minute.

Patentansprüche

1. System zum Vergleichen und Zusammenpassen nicht vorhersagbarer Codes, die durch getrennte Computer erzeugt wurden, umfassend:
einen ersten Computer (20), der zur Erzeugung eines ersten nicht vorhersagbaren Codes (40) auf der Basis einer ersten dynamischen Variablen (30) und einer statischen Variablen (10) betätigbar ist, eine erste Takteinrichtung zur Definierung der ersten dynamischen Variablen (30) entsprechend einem ersten Zeitintervall, während dessen die statische Variable in den ersten Computer (20) eingegeben wird,
einen zweiten Computer (50), der zur Erzeugung eines zweiten nicht vorhersagbaren Codes (70) auf der Basis einer zweiten dynamischen Variablen (60) und der statischen Variablen (10) betätigbar ist, eine zweite Takteinrichtung zur Definierung der zweiten dynamischen variablen (60) entsprechend einem zweiten Zeitintervall, während dessen die statische variable (10) in den zweiten Computer (50)

eingegeben wird, und Einrichtungen (80) zum Vergleichen des ersten und zweiten nicht vorhersagbaren Codes (40, 70), um eine Übereinstimmung festzustellen,
dadurch **gekennzeichnet,**
daß das zweite Zeitintervall eine zentrale Zeitzelle umfaßt, welche eine vorbestimmte Dauer besitzt, und eine oder mehrere Zeitzellen, von denen jede eine vorbestimmte Dauer besitzt und die die zentrale Zelle umgrenzen, und
daß die zweite Takteinrichtung jeweilige Werte der zweiten dynamischen Variablen (60) für jede Zeitzelle definiert, wodurch der zweite Computer jeweilige Werte des zweiten nicht vorhersagbaren Codes für jede der Zeitzellen für den Vergleich mit dem ersten nicht vorhersagbaren Code liefert.

2. System nach Anspruch 1, bei dem Einrichtungen zum Synchronisieren der ersten Takteinrichtung und der zweiten Takteinrichtung beim Übereinstimmen des ersten nicht vorhersagbaren Codes (40) mit einem der zweiten nicht vorhersagbaren Codes (70) vorgesehen sind.

3. System nach Anspruch 1 oder 2, bei dem die zentrale Zeitzelle das Datum und die Minute umfaßt, zu dem die einzigartige statische Variable in den zweiten Computer (50) eingegeben wird, wie durch die zweite Takteinrichtung definiert.

4. System nach Anspruch 1, 2 oder 3, bei dem die umgrenzenden Zeitzellen eine Zeitzelle umfassen, welche das Datum und die Minute unmittelbar vorausgehend der zentralen Zelle umfaßt.

5. System nach einem der vorhergehenden Ansprüche, bei dem die umgrenzenden Zeitzellen eine ausgewählte Zahl von Zeitzellen umfassen, die unmittelbar der zentralen Zelle vorausgehen, sowie eine ausgewählte Zahl von Zeitzellen, die unmittelbar der zentralen Zelle folgen.

6. System nach einem der vorhergehenden Ansprüche, bei dem die zentrale und umgrenzenden Zeitzellen derart gewählt sind, daß sie eine Dauer von einer Minute besitzen.

7. System nach einem der Ansprüche 2 bis 6, umfassend:
Zähleinrichtungen zum Zählen der Zeitdifferenz zwischen einer zentralen Zeitzelle und einer umgrenzenden Zeitzelle, aus der ein zusammenpassender zweiter nicht vorhersagbarer Code (70) erzeugt werden kann;
Summiereinrichtungen die mit den Zähleinrichtungen verbunden sind, um aufeinanderfolgende, von den Zähleinrichtungen gezählte Zeitdifferenzen zu summieren;
Speichereinrichtungen, die zum Speichern des Ausgangs der Summiereinrichtungen mit den Summiereinrichtungen verbunden sind; und
Schiebeeinrichtungen, die mit den Speichereinrichtungen verbunden sind, um eine zentrale Zelle und umgrenzende Zeitzellen, um die in den Speichereinrichtungen gespeicherten summierten Zeiten zu verschieben.

8. System nach Anspruch 7, umfassend:
zweite Speichereinrichtungen, die mit der Vergleichseinrichtung verbunden sind, um das Datum des letzten Vergleichs und der Übereinstimmungsbestimmung durch die Vergleichseinrichtung zu speichern;
zweite Zähleinrichtungen, die mit den zweiten Speichereinrichtungen verbunden sind, um die Zeitdifferenz zwischen dem gespeicherten Datum und dem Datum des gegenwärtigen Zugriffs zu dem zweiten Computer zu zählen;
Dividiereinrichtungen, die mit den zweiten Zähleinrichtungen verbunden sind, um die von den zweiten Zähleinrichtungen gezählte Zeitdifferenz durch einen ausgewählten Wert zu dividieren und um den Ausgang als eine erste Fensteröffnungszahl vorzuschreiben;
Fensteröffnungseinrichtungen, die mit den Dividiereinrichtungen und den Vergleichseinrichtungen verbunden sind, um so viele zusätzliche zweite nicht vorhersagbare Codes auf der Basis von so vielen zusätzlichen umgrenzenden Zeitzellen, die der ausgewählten Anzahl von umgrenzenden Zeitzellen unmittelbar vorhergehen und folgen, wie durch die erste Fensteröffnungszahl vorgeschrieben, zu berechnen.

9. System nach Anspruch 8, ferner umfassend:
Fühleinrichtungen, die mit der zweiten Takteinrichtung verbunden sind, um ein Rücksetzen der zweiten Takteinrichtung zu ermitteln;
dritte Speichereinrichtungen, die mit den Fühleinrichtungen verbunden sind, um das Auftreten eines ermittelten Rücksetzens der zweiten Takteinrichtung als eine ausgewählte zweite Fensteröffnungszahl vorzuschreiben und zu speichern; und
zweite Fensteröffnungseinrichtungen, die mit den dritten Speichereinrichtungen verbunden sind, um so viele zusätzliche nicht vorhersagbare Codes auf der Basis von so vielen zusätzlichen umgrenzenden Zeitzellen, die unmittelbar den zusätzlichen umgrenzenden Zeitzellen vorausgehen und diesen folgen, wie durch die

zweite Fensteröffnungszahl vorgeschrieben, zu berechnen.

10. System nach einem der vorhergehenden Ansprüche, bei dem der erste oder der zweite Computer (20, 50) einen Mikroprozessor umfaßt, bei dem ein Algorithmus in einem flüchtigen dynamischen Speicher mit einer Stromversorgungseinrichtung gespeichert ist, die bei Unterbrechung alle Daten einschließlich wenigstens des Algorithmus und der statischen Variablen zerstört.

11. System nach einem der vorhergehenden Ansprüche, bei dem der erste Computer (20) und die erste Takteinrichtung in einer Karte von etwa der gleichen Größe wie eine Kreditkarte aufgenommen sind.

12. System nach einem der vorhergehenden Ansprüche, bei dem der erste Computer (50) Einrichtungen (44) zur visuellen Anzeige des gegenwärtig erzeugten, nicht vorhersagbaren Codes (40) umfaßt.

13. System nach Anspruch 10, bei dem die Karte eine Länge von ungefähr 84 mm (3,3 Zoll), eine Breite von ungefähr 53 mm (2,1 Zoll) und eine Dicke von ungefähr 1,8 mm (0,07 Zoll) besitzt.

14. System nach Anspruch 12, bei dem die übliche Anzeigeeinrichtung (44) eine Flüssigkristallanzeige ist.

15. Verfahren zum Synchronisieren der Zeitdefinition von dynamischen Variablen (30, 60) in einem System zum Vergleichen nicht vorhersagbarer Codes (40, 70), die durch getrennte Takteinrichtungen entsprechend der Zeit erzeugt wurden, wobei die Codes dann übereinstimmen, wenn die dynamischen Variablen übereinstimmen, umfassend die folgenden Schritte:
Eingeben einer statischen variable (10) in einen ersten Computer (20), der einen vorbestimmten Algorithmus umfaßt;
Verwenden des Algorithmus des ersten Computers (20), um einen ersten nicht vorhersagbaren Code (40) auf der Basis der statischen Variablen (10) und einer ersten dynamischen Variablen (30) zu berechnen, die durch ein erstes Zeitintervall definiert ist, in dem das Eingeben entsprechend einem ersten Takt erfolgte;
unabhängiges Eingeben der statischen Variablen (10) und des ersten nicht vorhersagbaren Codes (40) in einen zweiten Computer (50), der den vorbestimmten Algorithmus umfaßt;
Verwenden des Algorithmus des zweiten Computers (50) zur unabhängigen Berechnung eines zweiten nicht vorhersagbaren Codes (70) auf der Basis der statischen Variablen (10) und einer zweiten dynamischen Variablen (60), die durch ein zweites Zeitintervall definiert ist, in dem der Schritt des Eingebens entsprechend einer zweiten Takteinrichtung erfolgte; und
Vergleichen des ersten und des zweiten nicht vorhersagbaren Codes (40, 70), um eine Übereinstimmung festzustellen;
dadurch **gekennzeichnet,**
daß das zweite Zeitintervall eine zentrale Zeitzelle und eine oder mehrere umgrenzende Zeitzellen umfaßt; und
daß der Algorithmus des zweiten Computers (50) zur unabhängigen Berechnung einer Vielzahl von zweiten nicht vorhersagbaren Codes (70) auf der Basis der statischen Variablen (10) und zweiten dynamischen Variablen (60), die durch die Zeitzellen definiert sind, verwendet wird; und
Feststellen wenn eine Übereinstimmung zwischen dem ersten nicht vorhersagbaren Code (40) und einem der zweiten nicht vorhersagbaren Codes (50) auftritt.

16. Verfahren nach Anspruch 15, ferner umfassend die folgenden Schritte:
Zählen der Zeitdifferenz zwischen einer zentralen Zeitzelle und einer umgrenzenden Zeitzelle, woraus ein übereinstimmender zweiter nicht vorhersagbarer Code erzeugt werden kann;
Summieren aufeinanderfolgender Zeitdifferenzen, die während des Schrittes des Zählens gezählt wurden;
Speichern der summierten aufeinanderfolgenden Zeitdifferenzen; und
verschieben der zentralen und umgrenzenden Zeitzellen um die summierten aufeinanderfolgenden Zeitdifferenzen.

17. Verfahren nach Anspruch 16, ferner **gekennzeichnet,** durch die folgenden Schritte:
Speichern des Datums des letzten Vergleichs und der Feststellung einer Übereinstimmung;
Zählen der Zeitdifferenz zwischen dem gespeicherten Datum und dem Datum des gegenwärtigen Zugriffs in den zweiten Computer;
Dividieren der während des Schrittes des Zählens des Unterschieds der Datumsangaben gezählten Differenz durch einen ausgewählten Wert und Vorschreiben des Ausgangs als eine erste Fensteröffnungszahl; und Berechnen von so vielen zusätzlichen zweiten nicht vorhersagbaren Codes (70) auf der Basis von so vielen zusätzlichen umgrenzenden Zeitzellen unmit-

teilbar vorhergehend und nachfolgend der ausgewählten Anzahl von umgrenzenden Zellen, wie durch die erste Fensteröffnungszahl vorgeschrieben.

18. Verfahren nach Anspruch 17, umfassend die folgenden Schritte:
Ermitteln eines Rücksetzens der zweiten Takteinrichtung;
Vorschreiben und Speichern des Auftretens eines ermittelten Rücksetzens der zweiten Takteinrichtung als zweite ausgewählte Fensteröffnungszahl; und
Berechnen von so vielen zusätzlichen zweiten nicht vorhersagbaren Codes (70) auf der Basis von so vielen zusätzlichen umgrenzenden Zeitzellen, die unmittelbar den zusätzlichen umgrenzenden Zeitzellen vorausgehen und diesen folgen, wie durch die zweite Fensteröffnungszahl vorgeschrieben.

19. Verfahren nach Anspruch 15, bei dem die zentralen und die umgrenzenden Zeitzellen derart ausgewählt sind, daß sie eine Minute Dauer haben.

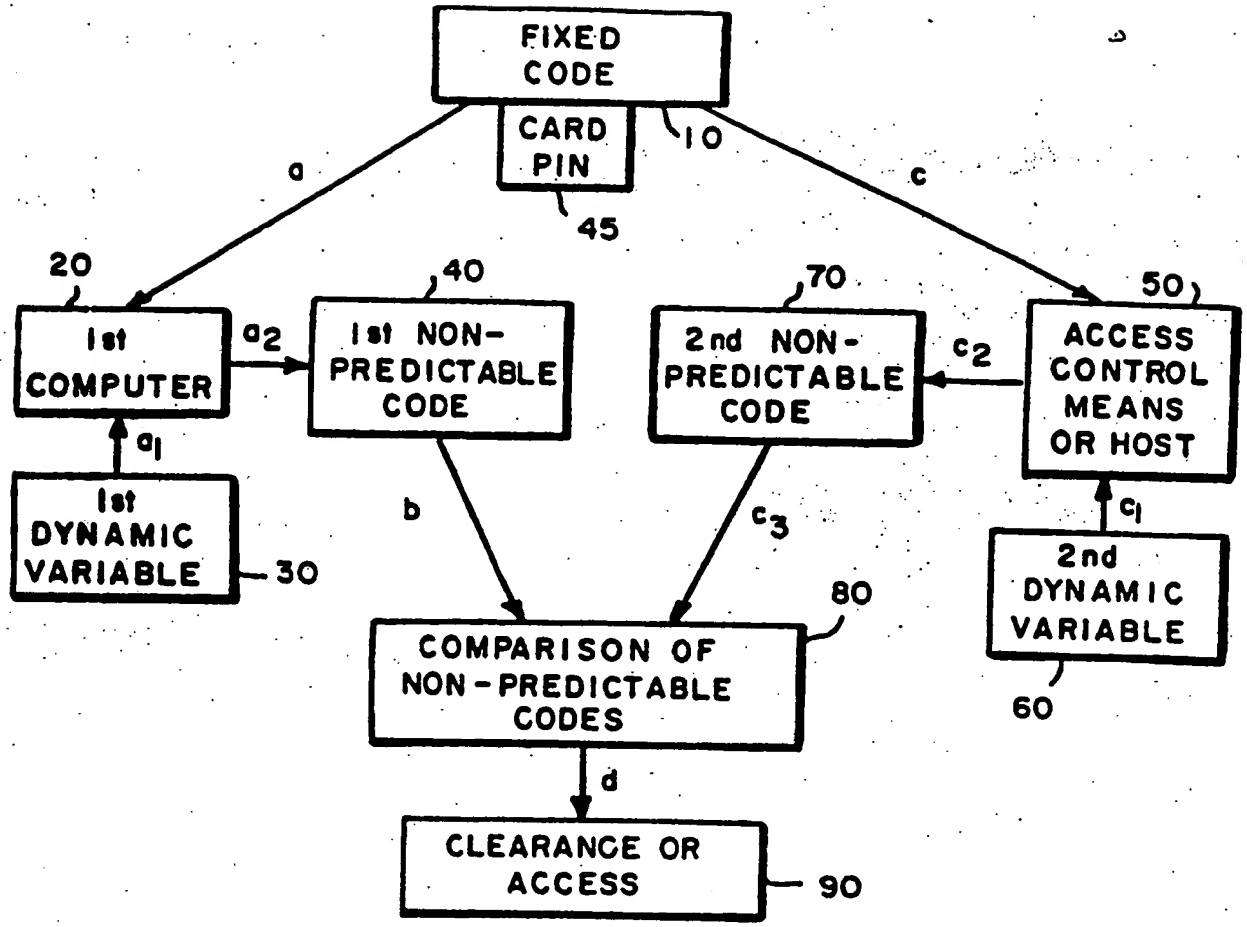
FIXED CODE
CARD PIN
10
45
a
c
20
40
70
50
1st COMPUTER
a2
1st NON-PREDICTABLE CODE
2nd NON-PREDICTABLE CODE
c2
ACCESS CONTROL MEANS OR HOST
a1
1st DYNAMIC VARIABLE
30
b
c3
c1
2nd DYNAMIC VARIABLE
60
80
COMPARISON OF NON-PREDICTABLE CODES
d
CLEARANCE OR ACCESS
90

FIG. 1

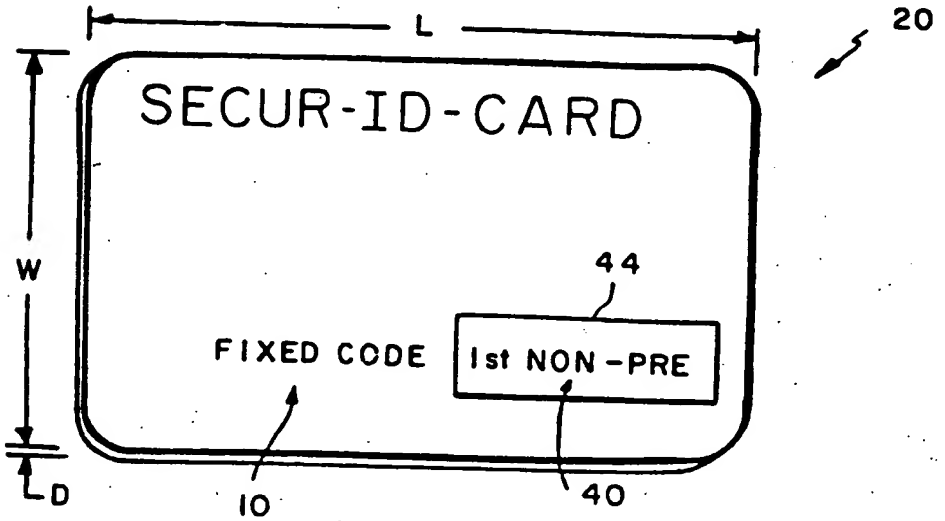
L
20
SECUR-ID-CARD
W
44
FIXED CODE
1st NON-PRE
D
10
40

FIG. 2

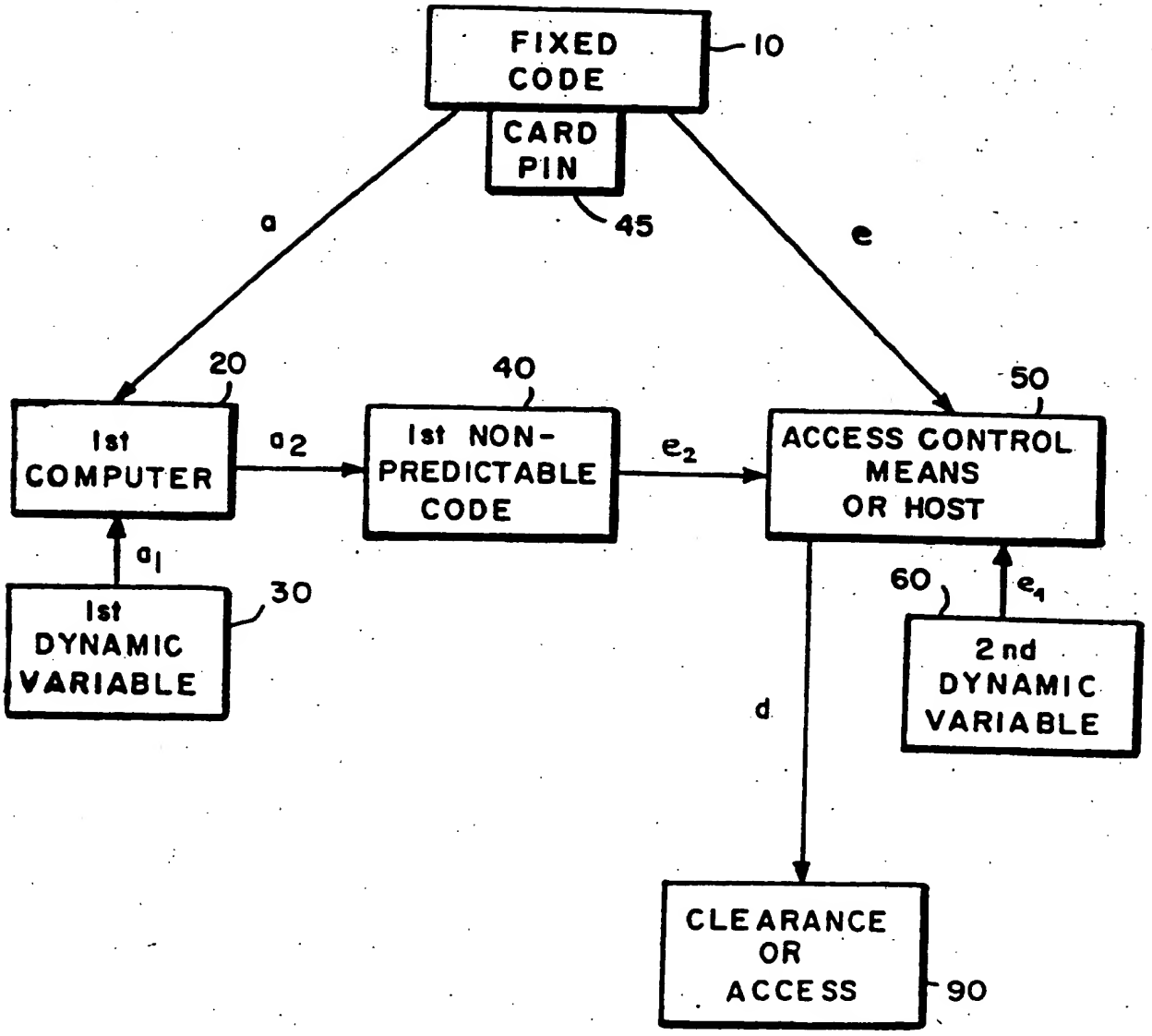
FIXED CODE
10
CARD PIN
45
a
e
20
40
50
1st COMPUTER
a_2
1st NON-PREDICTABLE CODE
e_2
ACCESS CONTROL MEANS OR HOST
a_1
1st DYNAMIC VARIABLE
30
60
e_1
2nd DYNAMIC VARIABLE
d
CLEARANCE OR ACCESS
90

FIG. 1A

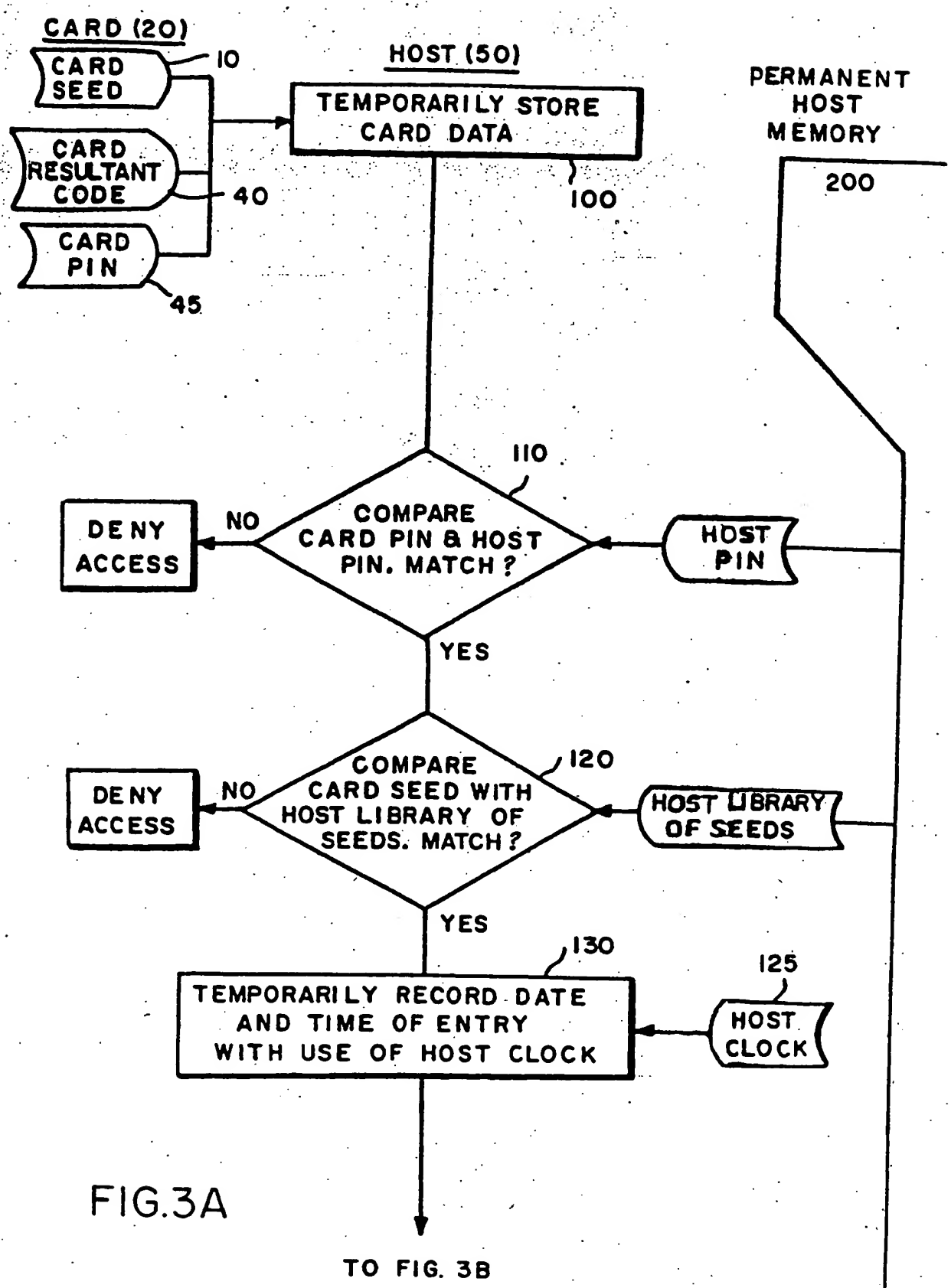
CARD (20)
CARD SEED
10
CARD RESULTANT CODE
40
CARD PIN
45
HOST (50)
TEMPORARILY STORE CARD DATA
100
PERMANENT HOST MEMORY
200
110
COMPARE CARD PIN & HOST PIN. MATCH ?
NO
DENY ACCESS
HOST PIN
YES
120
COMPARE CARD SEED WITH HOST LIBRARY OF SEEDS. MATCH ?
NO
DENY ACCESS
HOST LIBRARY OF SEEDS
YES
130
TEMPORARILY RECORD DATE AND TIME OF ENTRY WITH USE OF HOST CLOCK
125
HOST CLOCK
TO FIG. 3B

FIG.3A

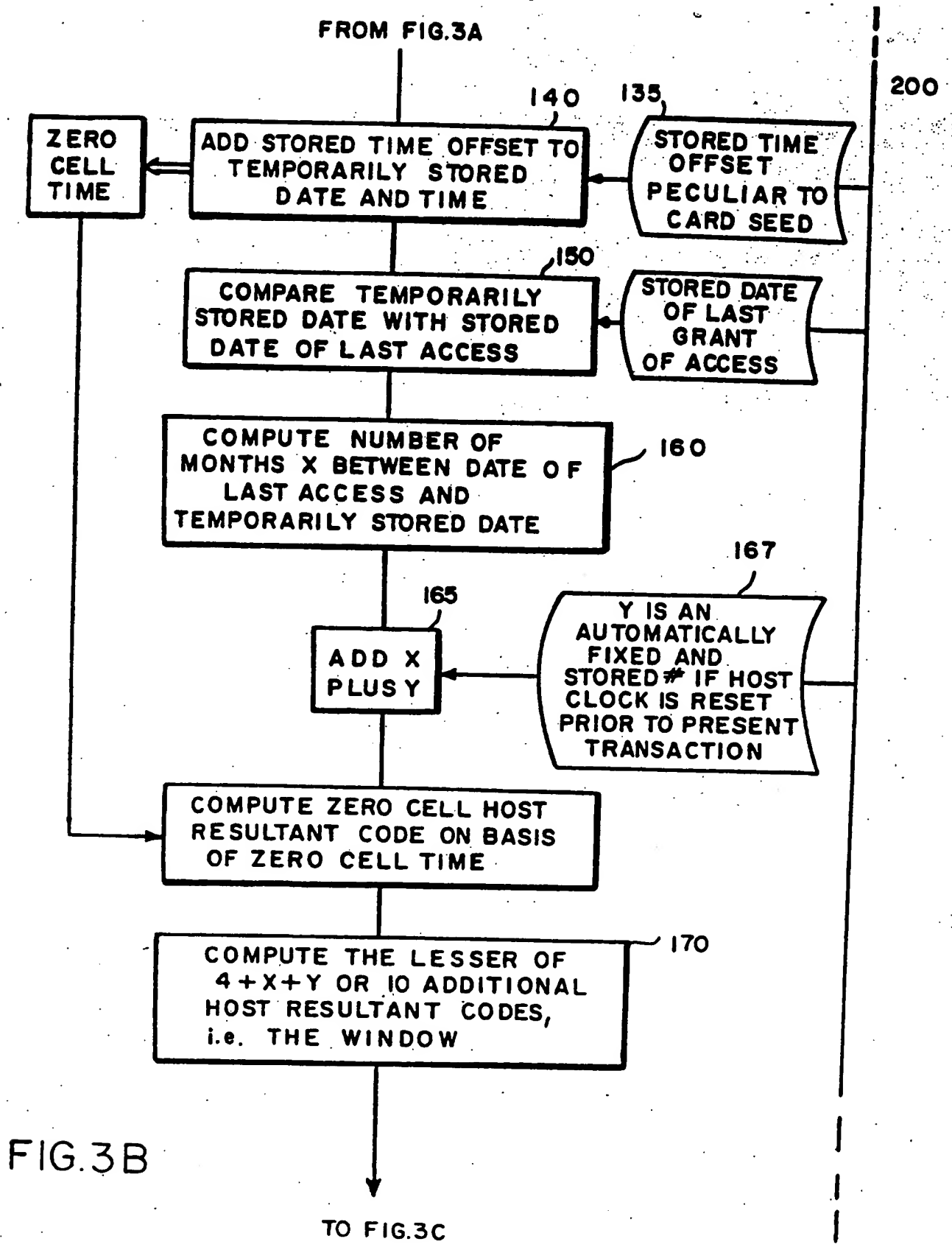
FROM FIG.3A
200
140
135
ZERO CELL TIME
ADD STORED TIME OFFSET TO TEMPORARILY STORED DATE AND TIME
STORED TIME OFFSET PECULIAR TO CARD SEED
150
COMPARE TEMPORARILY STORED DATE WITH STORED DATE OF LAST ACCESS
STORED DATE OF LAST GRANT OF ACCESS
COMPUTE NUMBER OF MONTHS X BETWEEN DATE OF LAST ACCESS AND TEMPORARILY STORED DATE
160
167
165
ADD X PLUS Y
Y IS AN AUTOMATICALLY FIXED AND STORED # IF HOST CLOCK IS RESET PRIOR TO PRESENT TRANSACTION
COMPUTE ZERO CELL HOST RESULTANT CODE ON BASIS OF ZERO CELL TIME
170
COMPUTE THE LESSER OF 4+X+Y OR 10 ADDITIONAL HOST RESULTANT CODES, i.e. THE WINDOW
TO FIG.3C

FIG.3B

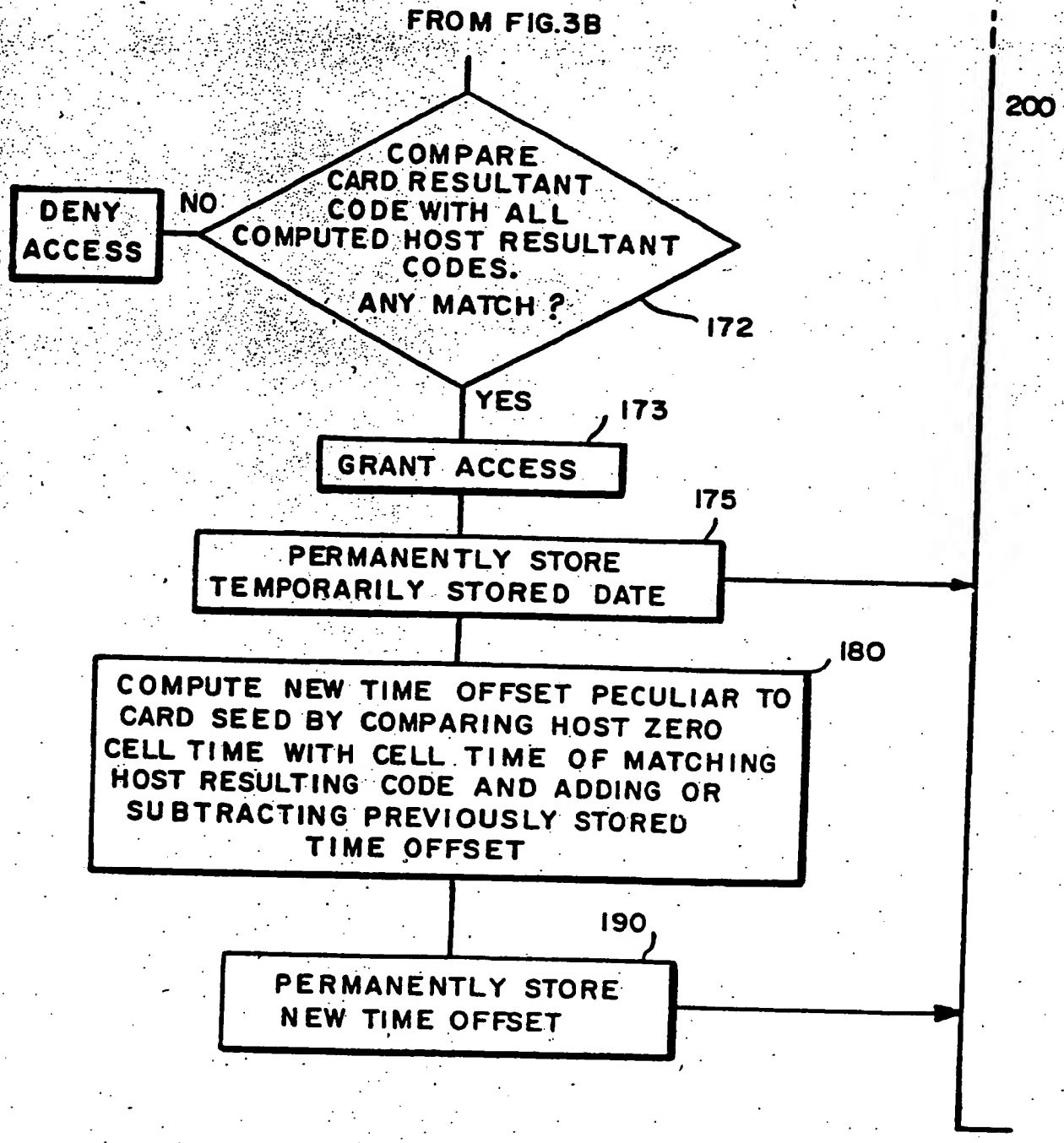
FROM FIG.3B
COMPARE CARD RESULTANT CODE WITH ALL COMPUTED HOST RESULTANT CODES. ANY MATCH ?
172
NO
DENY ACCESS
YES
173
GRANT ACCESS
175
PERMANENTLY STORE TEMPORARILY STORED DATE
180
COMPUTE NEW TIME OFFSET PECULIAR TO CARD SEED BY COMPARING HOST ZERO CELL TIME WITH CELL TIME OF MATCHING HOST RESULTING CODE AND ADDING OR SUBTRACTING PREVIOUSLY STORED TIME OFFSET
190
PERMANENTLY STORE NEW TIME OFFSET
200

FIG.3C

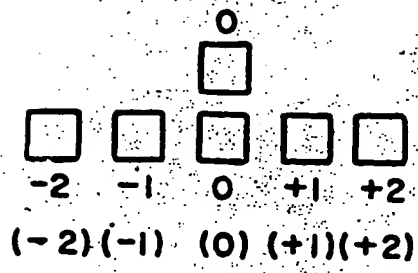

FIG.4

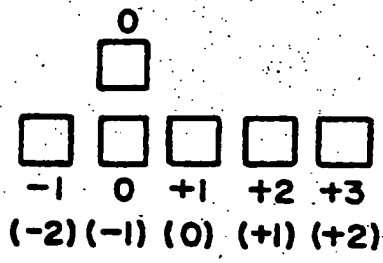

FIG.5

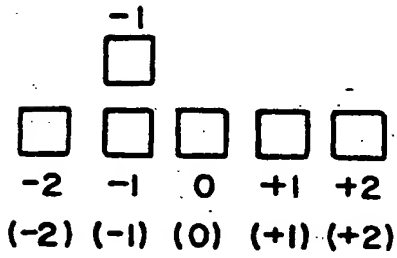

FIG.6

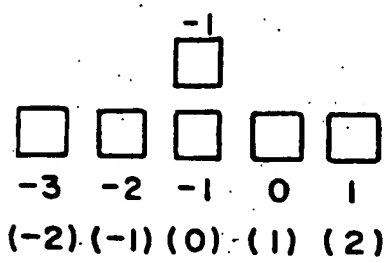

FIG.7

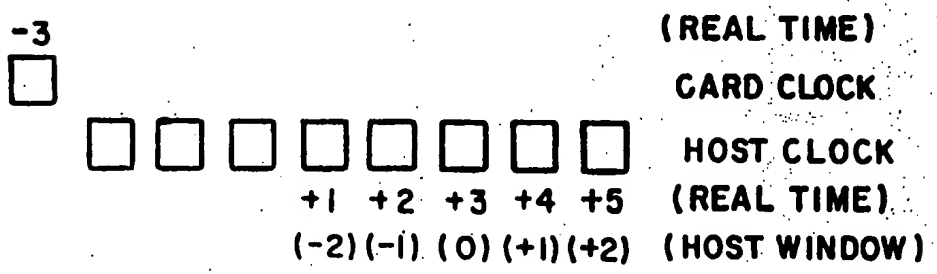

FIG.8

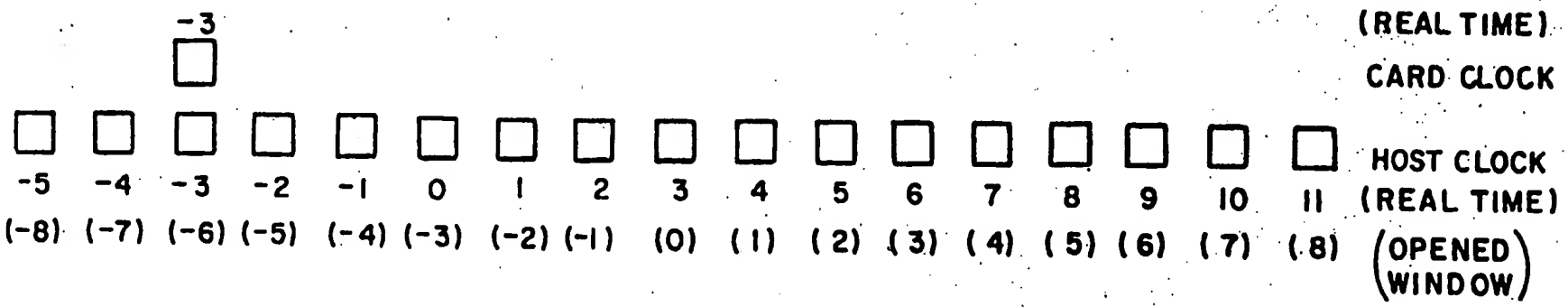

FIG.9

EP 0 234 100 B1